

Nächste Station Cloud: Wie Cloud4Rail den Plattform-Markt für Europas Bahnen mobilisiert

Die DB InfraGO verantwortet Betrieb, Instandhaltung und Ausbau der deutschen Schieneninfrastruktur. Das Projekt Cloud4Rail ist ein wesentlicher Schritt in Richtung eines zukunftsfähigen, digitalisierten Bahnbetriebs. Ziel ist die Entwicklung einer funktional sicheren und zertifizierbaren streckenseitigen Edge- und Cloud-Infrastruktur, die den digitalen Wandel im Bahnsystem maßgeblich vorantreibt.



Modulare IT-Plattformen als Grundlage eines digitalisierten Bahnsystems

Die deutsche Sektorinitiative „Digitale Schiene Deutschland“ (DSD) zielt darauf ab, die Chancen der Digitalisierung optimal zu nutzen, um Kapazität, Qualität und Effizienz des Bahnsystems signifikant zu steigern. Als Basis hierfür treibt die DSD den Roll-out von digitalen Stellwerken und des European Train Control Systems (ETCS) in Deutschland voran. Darauf aufbauend wird die Leit- und Sicherungstechnik zu einer kapazitätssteigernden zugzentrischen Logik (sog. „Moving Block“-Ansatz) weiterentwickelt, es wird eine künstliche Intelligenz (KI) basierte zentrale Disposition des Bahnbetriebs in Echtzeit entwickelt und eine Automatisierung des Bahnbetriebs bis hin zum vollautomatisierten Fahren (sog. Grad of Automation 4) angestrebt.

Eine wesentliche Voraussetzung für die Einführung der genannten Technologien ist die Umstellung des Bahnsystems auf die Nutzung einer zukunftsweisenden IT-Systemarchitektur mit modularen IT-Plattformen. Ein erster Schritt ist hierbei eine standardisierte Trennung von bahnbetrieblichen Anwendungen (z. B. digitalen Stellwerksfunktionen) von darunterliegenden IT-Plattformen, wie er in anderen Mobilitätssektoren bereits vollzogen wurde. Vorteile hiervon sind u. a. die Entkopplung der sehr unterschiedlichen Lebenszyklen von Bahnanwendungen und IT-Plattformen, bessere Nutzung von Standardlösungen und Trends im IT-Cloud-Bereich für den

Bahnsektor und die Schaffung eines größeren Ökosystems von Anwendungs- und Plattform-Anbietern. Auch ist der angestrebte Ansatz eine Grundlage für effiziente Georedundanz in einem hochresilienten Bahnsystem.

Die Arbeiten an diesem wesentlichen Paradigmenwechsel im Bahnsystem haben 2019 in Kooperation der Initiativen RCA (Reference Command-Control and Signalling Architecture) und OCORA (Open CCS On-board Reference Architecture) unter dem Titel „Safe Computing Platform“ begonnen [1], komplementiert durch F&E-Projekte wie „Sil4Cloud“ [2]. Später wurden diese Arbeiten und konkret die Spezifikation von Architektur und standardisierten Schnittstellen in das Europe's Rail Joint Undertaking (ERJU) [3] überführt.

Das Projekt Cloud4Rail setzt diese Arbeiten nun entscheidend fort, indem es eine konkrete, detaillierte Lösungsarchitektur mit maximaler Nutzung von State of the Art-Technologien für den zuvor genannten IT-Plattform-Ansatz entwickelt. Die Umsetzbarkeit dessen wird in einer weltweit ersten Referenzimplementierung und einem Demonstrator nachgewiesen. Hierbei ist das Projekt fortlaufend mit den Arbeiten des ERJU synchronisiert bzw. die wesentlichen Erkenntnisse fließen wieder dort ein.

In Cloud4Rail verfolgter Architekturansatz

Neben den zuvor genannten Designparadigmen einer modularen IT-Plattform für den Bahnbetrieb, hat sich Cloud4Rail noch



Dr. Patrick Marsch

Leiter Konnektivitäts-, IT- und Datenplattformen und IT/OT Security, Digitale Schiene Deutschland, DB InfraGO AG

Patrick.Marsch@deutschebahn.com



Alexander Heine

Leiter IT- und Datenplattformen und -dienste, Digitale Schiene Deutschland, DB InfraGO AG

Alexander.Heine@deutschebahn.com



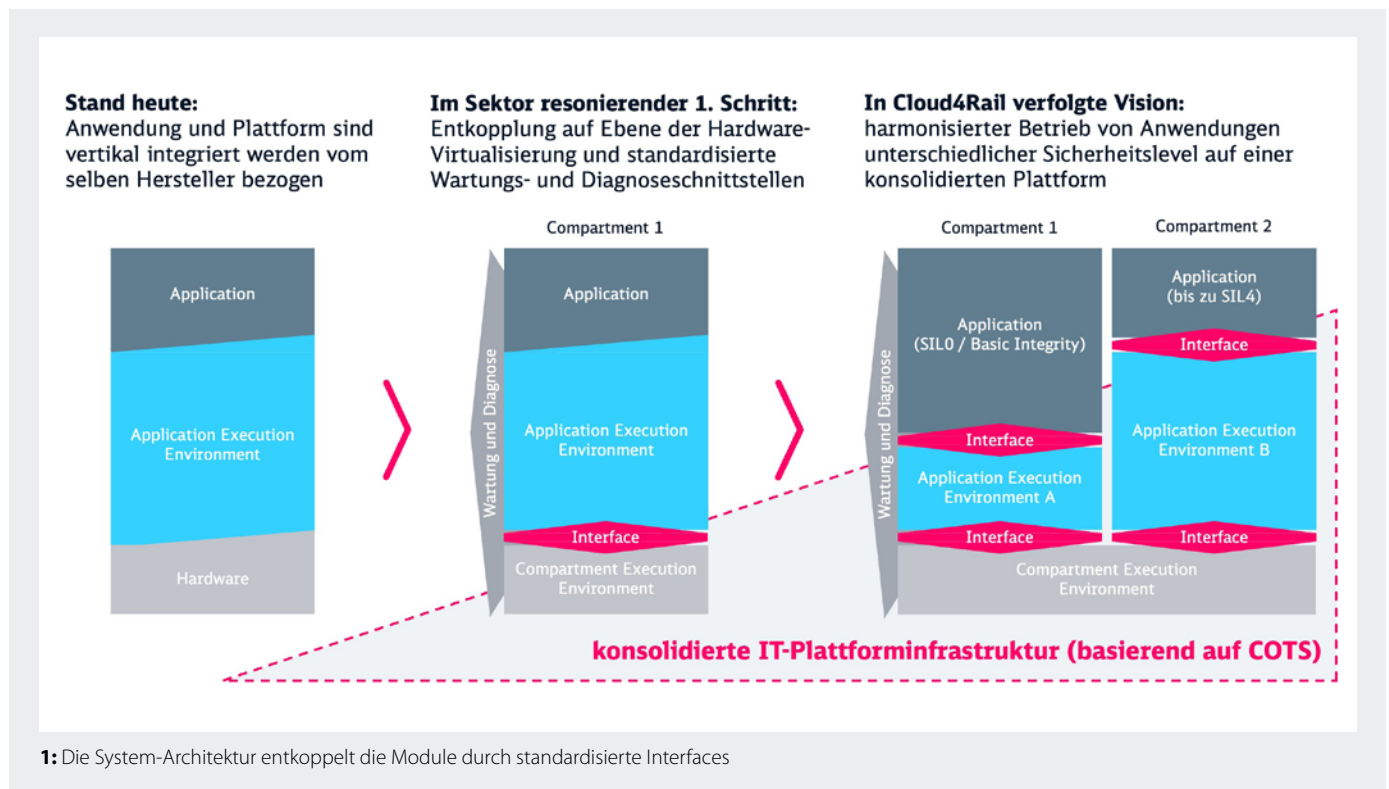
Wolfgang Albert

IT-System & Plattform Architekt, IT- und Datenplattformen und -dienste, Digitale Schiene Deutschland, DB InfraGO AG

Wolfgang.Albert@deutschebahn.com

Modulare IT-Plattformen, die eine effiziente Zulassung ermöglichen, sind Grundlage für die digitale, europäische Bahn von morgen.





weitere Designziele für die angestrebte Lösungsarchitektur gesetzt: So soll z.B. explizit ermöglicht werden, dass Anwendungen verschiedener Sicherheitslevel auf einer konsolidierten IT-Plattform betrieben werden. Ferner steht eine Reduktion der sektorspezifischen Komplexität, eine Vereinfachung des Betriebes und der Wartbarkeit sowie eine Erhöhung der Widerstandsfähigkeit der Plattform im Vordergrund. Eine wesentliche Anforderung an die Cloud4Rail-Architektur ist die effiziente Abnahme und Zulassung der Plattformumsetzung.

Cloud4Rail ist eingebettet in das europäische Cloud-Edge-Continuum 8ra des IPCEI-CIS (Important Project of Common European Interest - Next Generation Cloud Infrastructure and Services) [4] und spielt eine zentrale Rolle dabei, die spezifischen Anforderungen des Bahnbetriebs sowie anderer sicherheitskritischer Industrien in die Arbeiten an einer europäischen Cloud-Edge-Referenzarchitektur einzubringen. Diese Integration verankert die Anforderungen sicherheitskritischer Anwendungen, die im Bahnbereich unerlässlich sind, in den zukünftigen Industrie-Cloud Lösungen. Dadurch wird sichergestellt, dass die europäische Cloud-Infrastruktur auch den hohen Sicherheitsstandards des Schienenverkehrs gerecht wird.

In Bild 1 ist der High-Level-Ansatz der konkreten Umsetzung der Safe Computing Platform (SCP) in Cloud4Rail abgebildet. Dieses Diagramm zeigt auf, wie Commercial-off-the-Shelf (COTS) Industrieserver als entkoppelte Basis einer Ausführungsumgebung für sichere Anwendungen zur Verfügung stehen. Auf dieser Ausprägung der SCP ist es möglich, eine nicht sichere Anwendung auf derselben Hardware zusammen mit einer sicherheitskritischen Anwendung (bis SIL 4), z.B. in separaten virtuellen Maschinen (VMs) zu betreiben.

Die Safe Computing Platform muss neben der funktionalen Sicherheit auch den höchsten Anforderungen an Cybersicherheit gerecht werden. Dazu gehört zum Beispiel die Fähigkeit, regelmäßige Sicherheitsupdates effizient durchführen zu können. Eine besondere Herausforderung besteht in diesem Zusammenhang in der modularen Nachweisführung für die Zulassung im Bahnbetrieb. Die Plattform muss so gestaltet sein, dass sie kontinuierlich aktualisiert und erweitert werden kann, ohne dass bestehende Anwendungen neu zugelassen werden müssen, oder der Aufwand dafür stark reduziert bzw. automatisiert wird.

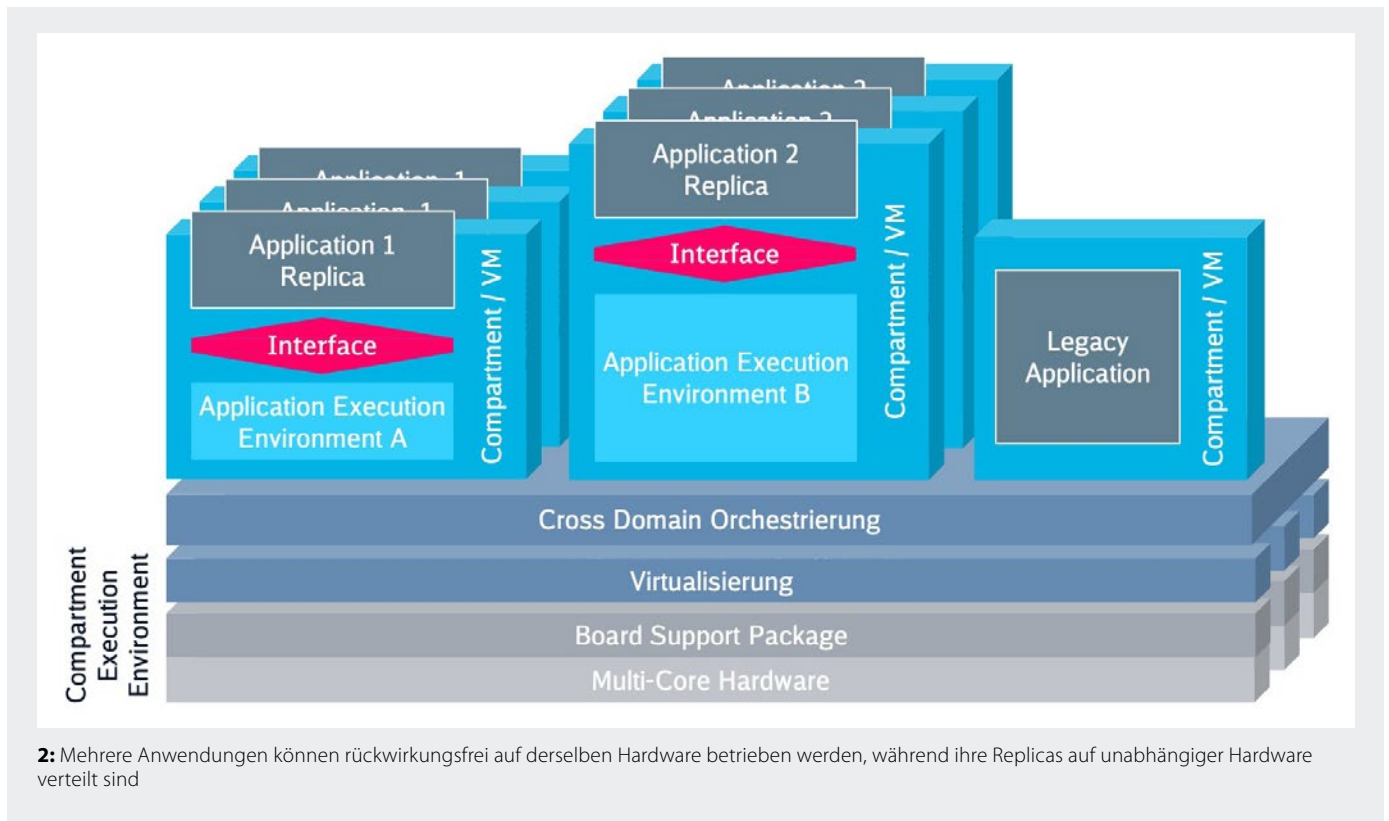
Kernkomponenten und Technologien

Die Architektur der Safe Computing Platform basiert auf einer modularen Struktur,

die eine strikte Trennung zwischen Anwendungen, Middleware und Hardware ermöglicht. Dynamische Kopplung sowie der Einsatz definierter Schnittstellen erlauben den Austausch jeder Komponente. Diese Trennung ist essenziell, um die unterschiedlichen Lebenszyklen jeder Komponente zu berücksichtigen und fortlaufende technologische Entwicklungen nutzen zu können, ohne die Integrität und Sicherheit des Gesamtsystems zu gefährden. Ein weiterer zentraler Aspekt dieser Architektur ist die von Grund auf garantierte Rückwirkungsfreiheit. Diese gewährleistet, dass Änderungen oder Updates an einer Komponente keine unbeabsichtigten Auswirkungen auf andere Komponenten sowie auf das Gesamtsystem haben können. Durch strikte Trennung und definierte Schnittstellen können neue Implementierungen oder Anpassungen isoliert vorgenommen werden. Die Stabilität und Sicherheit des Systems bleiben erhalten. Rückwirkungsfreiheit ist somit entscheidend für eine kontinuierliche Weiterentwicklung und Wartung der Plattform ohne das Risiko unerwarteter Fehlfunktionen.

Die drei Modul-Ebenen

Der Aufbau der Safe Computing Platform ist in drei Modulebenen unterteilt wie Bild 1 zeigt. Innerhalb jeder Ebene kön-



nen die darin enthaltenen Elemente und Anwendungen unter Einhaltung der Safety- und Security-Vorgaben ausgetauscht werden. Dies gewährleistet maximale Flexibilität, Stabilität, Zuverlässigkeit und Wartungsfreundlichkeit des Gesamtsystems. Im Folgenden werden die verschiedenen architektonischen Ebenen näher erläutert:

1. Compartment Execution Environment:

Die unterste Ebene wird als Compartment Execution Environment bezeichnet. Sie stellt die physikalischen Ressourcen bereit und separiert diese in Compartments. Durch Virtualisierung können mehrere Compartments als Virtuelle Maschinen (VMs) auf einem einzigen physischen System betrieben werden. Da die Compartments rückwirkungsfrei voneinander sind, können so nicht sichere Anwendung auf derselben Hardware zusammen mit einer sicherheitskritischen Anwendung laufen.

Innerhalb der Compartments sind die beiden weiteren Ebenen enthalten.

2. Application Execution Environment:

Diese mittlere Ebene enthält die Betriebssysteme und Laufzeitumgebungen für die Anwendungen.

Im Kontext von sicherheitskritischen Anwendungen enthält diese Ebene ebenfalls die notwendigen Systemdienste, um den funktional sicheren Betrieb der Anwendungen zu gewährleisten. Dies beinhaltet beispielsweise Replicamanagement und -überwachung dezentral über mehrere Compartments sowie die Unterstützung funktional sicherer Kommunikation.

Im Sinne der in RCA und OCORA definierten Safe Computing Plattform stellt diese Ebene die plattformunabhängigen Application Programming Interfaces (PI API) für sicherheits- und nicht sicherheitskritische funktionale Anwendungen zur Verfügung.

3. Application:

Als oberstes liegt die Ebene der funktionalen Anwendungen auf der Plattform. Hier werden sicherheitskritische Anwendungen bis zu SIL 4 sowie nicht sicherheitskritische Anwendungen ausgeführt. Diese funktionalen Anwendungen bauen auf den plattformunabhängigen APIs auf, was sie portabel und interoperabel zwischen verschiedenen Plattformimplementierungen macht.

Die Trennung von Anwendungen durch Compartments garantiert durch die exklusive Zuweisung physischer Ressour-

cen, dass diese rückwirkungsfrei ausgeführt werden.

Der fehlerfreie Betrieb der Anwendungen wird über die Compartments hinweg überwacht. Auf erkannte Fehler wird durch vordefinierte Maßnahmen automatisch reagiert, um einen weiterhin stabilen und sicheren Zustand der Anwendung zu gewährleisten.

Bedeutung von Schnittstellen

Eindeutig definierte Schnittstellen zwischen jeder Ebene sind Voraussetzung für die Umsetzung der Ebenen durch verschiedene Anbieter. Gleichzeitig ermöglicht eine weitgehende Standardisierung die Portabilität und Interoperabilität zwischen verschiedenen Implementierungen der gleichen Ebene.

Cloud4Rail setzt dabei auf die in der ERJU System Pillar Computing Environment Domäne definierte Interfacelogik und detailliert diese weiter.

Im Sinne des IPCEI-CIS, das ein Multi-Provider Cloud-Edge Kontinuum ohne Bindung an einen einzelnen Anbieter anstrebt, visiert das Projekt Cloud4Rail offene und freie Standards an. Dabei werden bevorzugt existierende De-facto-Standards aus der Cloud-Technologie-Community zu Grunde gelegt, und es wird auf die Veröf-

fentlichung unter Open-Source-Lizenzen gesetzt. Die erarbeiteten Inhalte sollen, sofern sie einen positiven Markteffekt bewirken, auch in europäische Eisenbahnstandards oder innerbetriebliche Regelwerke einfließen.

Konfiguration und Überwachung sicherheitskritischer Anwendungen

Um auf nicht sicherheitszertifizierter COTS Hardware die Ausführung von sicherheitskritischen Applikationen zu ermöglichen, greifen entsprechende Application Execution Environments auf die parallele Ausführung mehrerer Applikationsinstanzen in Compartments auf unabhängige Hardwareressourcen zurück (siehe Bild 2). So wird vermieden, dass ein möglicher Ausfall einer Hardwareressource oder ein nötiger Neustart mehrere Applikationsinstanzen betrifft. Diese Replication wird durch die MooN (M-out-of-N) Konfiguration ausgedrückt. Das Application Execution Environment implementiert umfangreiche Systemdienste zur Orchestrierung und Kommunikation zwischen den Replica, die eine funktional sichere Ausführung überwachen bzw. nötige Maßnahmen wie Neustarts automatisch einleiten.

Testbetrieb zu realen Bedingungen

Referenzimplementierungen der verschiedenen Ebenen durch Partner werden durch das Projekt Cloud4Rail integriert und im Digitalen Testfeld Bahn der DB InfraGO im Erzgebirge unter realen bahnbetrieblichen Bedingungen erprobt. Diese Demonstration dient als Grundlage für technische Zielbilder der Bahninfrastruktur. Dabei werden die Verbindungen zwischen physischen Elementen, wie Weichen und Signalen, vollständig in das System integriert. Zusätzlich werden Last- und Ausfallszenarien sowie Georedundanz-Konzepte betrachtet, um die Robustheit und Zuverlässigkeit der Plattform herzuleiten. Auch werden sich wichtige Erkenntnisse für die spätere Zertifizierung und Zulassung des Gesamtsystems ableiten lassen.

Erstmals wird der Demonstrator Cloud-Konzepte zum harmonisierten Betrieb sowohl von lokalen als auch cloudbasierten Ressourcen umsetzen. Nur so können Betrieb und Wartung der IT-Landschaft zukunftssicher und effizient realisiert werden.

Eine europaweite Initiative

Eine weitreichende Kooperation mit verschiedenen Partnern aus der Industrie und Wissenschaft ist für das Vorhaben entscheidend. Da die Plattform als Blaupause für einen europaweiten Einsatz im Eisenbahnsektor dienen soll, ist das Projekt in das europäische Programm IPCEI-CIS eingebettet. Als digitalpolitisches Schlüsselprojekt der Europäischen Union sind mehr als 150 Partner aus 12 EU-Mitgliedstaaten an diesem Programm beteiligt. In enger Zusammenarbeit mit der Generaldirektion Kommunikationsnetze der Europäischen Kommission wird der Aufbau eines Multi-Provider Cloud-Edge-Kontinuums ohne Bindung an einzelne Anbieter vorangetrieben. So können im Projekt Cloud4Rail auch Technologiekonzepte aus anderen Industriesektoren, wie der Automobil- und Luftfahrtindustrie, adaptiert und weiterentwickelt werden.

Fazit

Cloud4Rail ist ein zukunftsweisendes Projekt, das die Digitalisierung des Bahnsystems auf ein neues Level heben wird. Die Entwicklung einer modularen, funktional sicheren IT-Plattform schafft in Zusammenarbeit mit Unternehmen aus verschiedenen Industriebereichen die Grundlagen für den effizienten und automatisierten europäischen Bahnbetrieb der Zukunft. Die DB InfraGO AG setzt mit der ersten streckenseitigen Referenzimplementierung einer solchen Plattform einen wichtigen Meilenstein auf dem Weg zu einer nachhaltigen und zukunftssicheren Bahninfrastruktur in Europa.

Cloud4Rail besitzt dabei einen klaren Fokus auf die Nutzung von etablierten Cloud-Standards für den Betrieb und die Wartung von Bahnanwendungen mit Anforderungen an funktionale Sicherheit. Die Architektur der IT-Plattform zeichnet sich durch die standardisierte Trennung in unabhängige Ebenen aus. Die Systemdienste zur Überwachung der funktionalen Sicherheit werden hierbei von der Anwendungslogik abstrahiert. Durch Nutzung offener, plattformunabhängiger APIs wird ein Mehranbietersystem ermöglicht und die Austauschbarkeit von Produkten gewährleistet. Am Ende ermöglichen automatisierte Prozesse die effiziente Zulassung des integrierten Gesamtsystems. ●

Literatur

- [1] OCORA, „Approach for a Generic Safe Computing Platform for Railway Applications.“ All documents in section TWS03. https://github.com/OCORA-Public/Publications/tree/3a97a9cb89ec2dbd1314dd98a6c1517c81fde5a2/00_OCORA%20Latest%20Publications/Latest%20Release (Abruf am 3.9.2024; 18:50 Uhr).
- [2] Deutsche Bahn AG, Siemens Mobility. Forschungsbericht SIL4 Data Center mit der Deutschen Bahn AG und Siemens Mobility. Oktober 2021. https://digitale-schiene-deutschland.de/Downloads_Mediathek/Report%20-%20SIL4%20Cloud.pdf (Abruf am 3.9.2024; 18:50 Uhr).
- [3] RCA/OCORA, „Specification of the PI API between Application and Platform.“ Collaboration among DB Netz AG, duagon AG, Nederlandse Spoorwegen, RTI, SBB Siemens Mobility GmbH, SNCF Voyageurs, SNCF Réseau, Sysgo GmbH, Thales, and Wind River. Juli 2022. https://github.com/OCORA-Public/Publications/blob/master/00_OCORA%20Latest%20Publications/Latest%20Release/OCORA-TWS03-030_SCP_Specification_of_the_PL_API_between_Application_and_Platform.pdf (Abruf am 3.9.2024; 18:50 Uhr).
- [4] IPCEI Next Generation Cloud Infrastructure and Services <http://ipcei-cis.eu/> (Abruf am 3.9.2024; 18:50 Uhr).

Summary

Next stop cloud: How Cloud4Rail is mobilising the platform market for Europe's railways

The European rail sector is undergoing the biggest transformation in its history, towards a high degree of digitalisation of rail operations. This is based on forward-looking, modular IT platforms, which are specified in Europe's Rail. The Cloud4Rail project complements this work with the design of a concrete solution architecture for a modular, safe and certifiable railway IT platform and demonstrates its feasibility.